Modular arithmetic

From Wikipedia, the free encyclopedia.

This article is about an algebra concept. See modulo for other uses.

Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value — the **modulus**. Modular arithmetic was introduced by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae* published in 1801.

One way to understand modular arithmetic is to consider "clock arithmetic": the arithmetic of hours on the clock face. If we begin at 7 o'clock and add 8 hours, then rather than ending at 15 o'clock (as in usual addition), we are at 3 o'clock. Likewise, if we start at noon and count off 7 hours three times (3 × 7), we end up at 9 o'clock (rather than 21). Essentially, when we reach 12, we start over; 12 is called the *modulus*, and so this is an example of arithmetic *modulo* 12.

Contents

- 1 The congruence relation
- 2 The ring of congruence classes
- 3 Remainders
- 4 Applications
- 5 References
- 6 See also
- 7 External links

The congruence relation

Two integers a, b are said to be **congruent** modulo n if their difference is a multiple of n. In this case, we write

$$a \equiv b \pmod{n}.$$

For instance,

$$38 \equiv 14 \pmod{12}$$

because $38 - 14 = 24$ which is a multiple of 12. For positive numbers, congruence can also be thought of as asserting that two numbers have the same remainder after dividing by the modulus n. So,

$$38 \equiv 14 \pmod{12}$$

because when divided by 12 both numbers give 2 as remainder.

Congruence is an equivalence relation, and the equivalence class of the integer a is denoted by $[a]_n = \{ \ldots, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \ldots\}$. This set of all integers congruent to a modulo n is called the **congruence class** or **residue class** of a modulo n, and is also denoted by $\hat{a}$.

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n}$$

then

$$a_1 + a_2 \equiv (b_1 + b_2) \pmod{n}$$

and

$$a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

This observation underpins modular arithmetic.

This is the prototypical example of a congruence relation.

The ring of congruence classes

One can then define formally an addition and multiplication on the set

$$\mathbf{Z}/n\mathbf{Z} = \{ [0]_n, [1]_n, [2]_n, \ldots, [|n|-1]_n \}$$

of all equivalence classes by the following rules:

- $[a]_n + [b]_n = [a + b]_n$
- $[a]_n \times [b]_n = [ab]_n$

In this way, $\mathbf{Z}/n\mathbf{Z}$ becomes a commutative ring with $|n|$ elements. For instance, in the ring $\mathbf{Z}/12\mathbf{Z}$, we have

$$[8]_{12} + [6]_{12} = [2]_{12}.$$

The notation $\mathbf{Z}/n\mathbf{Z}$ is used, because it is the factor ring of $\mathbf{Z}$ by the ideal $n\mathbf{Z}$ containing all integers divisible by n.

In terms of groups, the residue class $[a]_n$ is the coset of a in the quotient group $\mathbf{Z}/n\mathbf{Z}$, a cyclic group.

The set $\mathbf{Z}/n\mathbf{Z}$ has a number of important mathematical properties that make it the foundation of many different branches of mathematics.

Where $n = 0$, $\mathbf{Z}/n\mathbf{Z}$ does not have zero elements; rather, it is isomorphic to $\mathbf{Z}$, since $[a]_0 = \{a\}$. This seemingly counterintuitive special case follows from the definitions and is useful for example when discussing the characteristic of a ring.

Remainders

The notion of modular arithmetic is related to that of the remainder in division. The operation of finding the

remainder is known as the modulo operation and is sometimes written as "mod", so we write "14 **mod** 12 = 2". Note that this meaning of "mod" is subtly but significantly different from that introduced in this article; it is true to say "38 ≡ 14 (**mod** 12)" , but it is not true to say "38 = 14 **mod** 12" — 38 is congruent to 14 modulo 12, but the remainder of 14 divided by 12 is 2, not 38.

When working with modular arithmetic, we usually represent each equivalence class with its least non-negative member, which is called the *common residue*. This can be found using long division.

Applications

Modular arithmetic is referenced in number theory, group theory, ring theory, abstract algebra, cryptography, computer science, and the visual and musical arts.

It is one of the foundations of number theory, touching on almost every aspect of its study, and provides key examples for group theory, ring theory and abstract algebra.

In cryptography, modular arithmetic directly underpins public key systems such as RSA and Diffie-Hellman, as well as providing finite fields which underlie elliptic curves, and is used in and a variety of symmetric key algorithms including IDEA and RC4.

In computer science, modular arithmetic is often applied in operations involving binary numbers and other fixed-width, cyclic data structures. The modulo operation, as implemented in many programming languages and calculators, is an application of modular arithmetic that is often used in this context.

In the visual arts, modular arithmetic can be used to create artistic patterns based on the multiplication and addition tables modulo *n* (see external link, below).

In music, modular arithmetic is used in the consideration of the twelve tone equally tempered scale, where octave and enharmonic equivalency occurs (that is, pitches in a 1 : 2 or 2 : 1 ratio are equivalent, and C-sharp is the same as D-flat).

References

- Tom M. Apostol, *Introduction to Analytic Number Theory*, (1976) Springer-Verlag, New York. See in particular chapters 5 and 6 for a review of basic modular arithmetic.
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0262032937. Section 31.3: Modular arithmetic, pp.862–868.

See also

- Quadratic residue
- Legendre symbol
- Quadratic reciprocity
- Primitive root
- Topics relating to the group theory behind modular arithmetic:
  - Cyclic group
  - Multiplicative group of integers modulo n
- Other important theorems relating to modular arithmetic:
  - Chinese remainder theorem
  - Fermat's little theorem

- Lagrange's theorem

External links

- In this modular art (http://britton.disted.camosun.bc.ca/modart/jbmodart.htm) article, one can learn more about applications of modular arithmetic in music.
- Congruence (http://mathworld.wolfram.com/Congruence.html) from MathWorld.

Retrieved from "http://en.wikipedia.org/wiki/Modular_arithmetic"

Categories: Modular arithmetic | Ring theory | Group theory